APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: OBJECT-ORIENTED INSTRUCTION SET FOR RESOURCE-CONSTRAINED DEVICES

APPLICANT: JOSHUA B. SUSSER AND JUDITH E. SCHWABE

"EXPRESS MAIL" Mailing Label Number TB 888 891 432 US

Date of Deposit February 2, 1999

OBJECT-ORIENTED INSTRUCTION SET FOR RESOURCE-CONSTRAINED DEVICES

CROSS REFERENCE TO RELATED APPLICATIONS

The following applications are incorporated herein by reference in their entirety:

"Architecture-Neutral Exception Handling" and "Token-Based Linking," each naming Joshua B. Susser and Judith E. Schwabe as inventors, which are being filed concurrently with the present application; and

"Virtual Machine with Securely Distributed Bytecode Verification," naming Moshe Levy and Judy Schwabe as inventors, filed April 15, 1997.

In addition, an Appendix entitled "Java Card™ Virtual Machine Specification: Java Card Version 2.1" is attached to this application and forms a part of the present specification.

BACKGROUND

The present invention relates, in general, to object-oriented, architecture-neutral programs for use with

resource-constrained devices such as smart cards and the like.

A virtual machine is an abstract computing machine generated by a software application or sequence of instructions which is executed by a processor. The term "architecture-neutral" refers to programs, such as those written in the Java™ programming language, which can be executed by a virtual machine on a variety of computer platforms having a variety of different computer architectures. Thus, for example, a virtual machine being executed on a Windows™-based personal computer system will use the same set of instructions as a virtual machine being executed on a UNIX™-based computer system. The result of the platform-independent coding of a virtual machine's sequence of instructions is a stream of one or more bytecodes, each of which is, for example, a one-byte-long numerical code.

Use of the Java programming language has found many applications including, for example, those associated with Web browsers.

The Java programming language is object-oriented. In an object-oriented system, a "class" describes a collection of data and methods that operate on that data. Taken together, the data and methods describe the state of and behavior of an object.

Java also is verifiable such that, prior to execution of an application written in the Java programming language, a determination can be made as to whether any instruction sequence in the program will attempt to process data of an improper type for that bytecode or whether execution of bytecode instructions in the program will cause underflow or overflow of an operand stack.

A Java™ virtual machine executes virtual machine code written in the Java programming language and is designed for use with a 32-bit architecture. However, various resource-constrained devices, such as smart cards, have an 8-bit or 16-bit architecture.

Smart cards, also known as intelligent portable data-carrying cards, generally are made of plastic or metal and have an electronic chip that includes an embedded microprocessor to execute programs and memory to store programs and data. Such devices, which can be about the size of a credit card, typically have limited memory capacity. For example, some smart cards have less than one kilo-byte (1K) of random access memory (RAM) as well as limited read only memory (ROM), and/or non-volatile memory such as electrically erasable programmable read only memory (EEPROM). The limited architecture and memory make it impractical or impossible to implement the full Java Virtual Machine on the device.

Furthermore, smart cards come with a variety of processors and configurations. Thus, it is desirable to provide a platform-independent programming language that can be executed on such a resource-constrained device.

SUMMARY

In general, a verifiable, object-based, type-safe and pointer-safe instruction set is described for application software programs which can be downloaded to and executed on a range of resource-constrained devices.

According to one aspect, an application software program includes an object-oriented, verifiable, type-safe and pointer-safe sequence of instructions residing on a computer-readable medium. The program can be loaded to and executed by a resource-constrained device that is based on

an architecture of fewer than 32 bits, such as a 16-bit or 8-bit architecture.

According to another aspect, an application software program includes an object-oriented, verifiable, type-safe and pointer-safe sequence of instructions residing on a computer-readable medium. The program can be loaded to and executed by a resource-constrained device having random access memory with a capacity of no more than about 64K.

Various implementations include one or more of the following features. For example, each instruction can include an 8-bit operation code, and the sequence of instructions can be hardware platform-independent. In some implementations, the sequence includes instructions that were previously converted from at least one Java class file with at least some references to a constant pool transformed to inline data. For example, the instructions can include operation codes and operands. Some references to the constant pool can be inlined into operands, and some references to the constant pool can be inlined into operation codes.

Similarly, in some embodiments, the instructions can be executed by a device that supports multiple data types. The sequence of instructions can include data manipulation instructions each of which is specific to a particular data type. In some implementations, the data type associated with each data manipulation instruction is selected from among one of the following types: an 8-bit signed two's complement integer numeric type, a 16-bit signed two's complement integer numeric type and a 32-bit signed two's complement integer numeric type. Additionally, the instructions can be executed by a device that supports multiple reference types each of which is selected from among one of the following types: a class type, an interface

type and an array type. Furthermore, the program can include one or more composite instructions for performing an operation on a current object.

According to another aspect, a resource-constrained device includes memory for storing an application software program comprising an object-oriented, verifiable, type-safe and pointer-safe sequence of instructions. The device also includes a virtual machine implemented on a microprocessor. The virtual machine is capable of executing the sequence of instructions. In various embodiments, the device may be based on a limited architecture or may have a limited amount of memory. For example, in some implementations, the device includes random access memory having a capacity of no more than about 64K. In other embodiments, the microprocessor is based on an architecture of less than 32 bits, for example, a 16 or 8-bit architecture.

In other embodiments, an application-specific integrated circuit (ASIC) or a combination of a hardware and firmware can be used instead of a virtual machine running on a microprocessor.

In one particular application of the invention, the resource-constrained device is a smart card. The smart card can include a virtual machine implemented on a microprocessor, wherein the virtual machine is capable of executing a sequence of instructions such as those described above.

According to another aspect, methods are disclosed for using an application software program including an object-oriented, verifiable, type-safe and pointer-safe sequence of instructions. The software program can be received in a resource-constrained device having, for example, either limited memory or based on a limited architecture. The sequence of instructions then can be

executed on the resource-constrained device. In some implementations, the software program can be accessed over a computer network such as the Internet prior to downloading it onto the device. When the program is downloaded to the resource-constrained device, constant pool indices that appear in the received set of instructions can be transformed to corresponding data values.

Various implementations include one or more of the following advantages. By supporting many, although not all, of the features of the Java language and by using the same semantics as the Java class files, platform-independent virtual machine code can be written to be executed by a smart card or other resource-constrained device.

The instruction set can inline certain data, which would otherwise appear as part of a constant pool, directly into operation codes or operands. Thus, the instruction set itself can incorporate certain information that would otherwise be stored in and obtained from a constant pool if one were using the Java class file format. By inlining some of the information directly into the instruction set, the size of the constant pool can be reduced, which can help reduce the amount of memory required to store the constant pool and can improve the execution speed of the bytecode. In some cases, inlining the information directly into an operation code can reduce the number of operands required for a particular instruction. Further inlining of information from a constant pool when the program is downloaded to the resource-constrained device can either eliminate the need to retain the constant pool on the device or reduce the size of the constant pool.

Other features such as composite instructions for performing operations on the current object and the explicit

handling of 16-bit arithmetic can further reduce the length of a bytecode program.

Other features and advantages will be readily apparent from the following detailed description, the accompanying drawings and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an exemplary system including a virtual machine residing on a smart card according to the invention.

FIG. 2 is a flow chart illustrating a method of providing executable code to a smart card according to the invention.

FIGS. 3A and 3B illustrate, respectively, an exemplary format of virtual machine instruction and an inner loop of execution of the virtual machine according to the invention.

FIGS. 4A and 4B are tables of an exemplary set of operation codes for the virtual machine listed in numerical order by operation code and in alphabetical order by mnemonic, respectively.

FIG. 5 is a list of data types which are supported by operation codes that exist for multiple data types according to the invention.

FIG. 6A illustrates the format of an "iipush" instruction according to the invention, and

FIG. 6B illustrates the format of a corresponding "ldc" instruction in the Java class file format.

FIG. 7A illustrates the format of a "checkcast" instruction in the Java class file format, and

FIG. 7B illustrates the format of a "checkcast" instruction according to the invention.

FIG. 8A illustrates the format of a family of "getfield_T" instructions according to the invention, and

FIG. 8B illustrates the format of a corresponding "getfield" instruction in the Java class file format.

FIG. 9A and 9B illustrate how an implementation program on the smart card prepares virtual machine code for installation on the smart card according to one embodiment of the invention.

FIGS. 10A and 10B illustrate alternative instructions for obtaining the same result according to the invention.

FIG. 11A illustrates bytecodes for carrying out a mathematical expression using the Java class file format, and

FIG. 11B illustrates bytecodes for carrying out the same mathematical expression according to the invention.

FIG. 12 is partial, non-exclusive list of resource-constrained devices with which the invention can be used.

DESCRIPTION

A verifiable, object-based, type-safe and pointer-safe instruction set is described below for application software programs which can be downloaded to and executed on a range of resource-constrained devices. Resource-constrained devices are generally considered to be those that are relatively restricted in memory and/or computing power or speed, as compared to conventional desktop computers and the like. Although the particular implementation discussed below is described in reference to a smart card, the invention can be used with other resource-constrained devices including, but not limited to, cellular telephones, boundary scan devices, field programmable

devices, personal digital assistants (PDAs) and pagers, as well as other miniature or small footprint devices.

Programs written with the instruction set described below are capable of being downloaded to and executed on resource-constrained devices having about sixty-four kilo-bytes (64K) of RAM or less. Some of the resource-constrained devices in which such programs can be executed may have no more than about sixteen kilo-bytes (16K) of RAM and others may have no more than about four kilo-bytes (4K) of RAM. Many of the devices also have limited amounts of other memory, such as no more than about twenty-four kilo-bytes (24K) of ROM, or no more than about 16K of non-volatile memory such as EEPROM. Similarly, some resource-constrained devices are based on an architecture designed for fewer than 32 bits. For example, some of the devices which can be used with the invention are based on an 8-bit or 16-bit architecture, rather than a 32-bit architecture. Of course, applications using the instruction set described below are upward compatible and can be executed, for example, on other Java platforms provided equivalent device support is present.

Referring to FIGS. 1 and 2, development of an applet for a resource-constrained device, such as a smart card 40, begins in a manner similar to development of other Java programs. In other words, a developer writes one or more JAVA classes (step 60) and compiles the source code with a JAVA compiler to produce one or more class files 10 (step 62). The applet can be run, tested and debugged, for example, on a workstation using simulation tools to emulate the environment on the card 40. When the applet is ready to be downloaded to the card 40, the class files 10 are converted to a converted applet (CAP) file 16 by a converter 14 (step 64). The converter 14 can be implemented as a Java

application being executed by a desktop computer. The converter 14 can accept as its input one or more export files 12 in addition to the class files 10 to be converted. An export file 12 contains naming or linking information for the contents of other packages that are imported by the classes being converted.

In general, the CAP file 16 includes all the classes and interfaces defined in a single Java package and is represented by a stream of 8-bit bytes. All 16-bit and 32-bit quantities are constructed by reading in two or four consecutive 8-bit bytes, respectively. Among other things, the CAP file 16 includes a constant pool component 18 which is packaged separately from a method component 20. The constant pool component 18 can include various types of constants, ranging from numerical literals known at compile time to method and field references which are resolved either when the program is downloaded to the smart card 40 or at the time of execution by the smart card. The method component 20 specifies the set of instructions to be downloaded to the smart card 40 and subsequently executed by the smart card. Further details of the structure of an exemplary CAP file 16 are discussed in the attached Appendix at pages 53 through 94 and in a publication by Sun Microsystems, Inc. entitled "Java Card Runtime Environment (JCRE) 2.1 Specification," (1998) which is incorporated herein by reference in its entirety.

After conversion, the CAP file 16 can be stored on a computer-readable medium 17 such as a hard drive, a floppy disk, an optical storage medium, a flash device or some other suitable medium.

The CAP file 16 then can be copied or transferred to a terminal 22 (step 66) such as a desktop computer with a peripheral card acceptance device (CAD) 24. In some

embodiments, the terminal 22 can be connected to a network (not shown), such as the Internet, a local area network (LAN) or a wide area network (WAN), which communicates with other computing devices such as a server. In such situations, the CAP file 16 can be accessed and transmitted to the terminal 22 over the network. The CAP file 16 also can be provided to the terminal 22 using a carrier wave, such as a network data transmission.

The CAD 24 allows information to be written to and retrieved from the smart card 40. The CAD 24 includes a card port (not shown) into which the smart card 40 can be inserted. Once inserted, contacts from a connector press against the surface connection area on the smart card 40 to provide power and to permit communications with the smart card, although, in other implementations, contactless communications can be used. The terminal 22 also includes an installation tool 26 which loads the CAP file 16 for transmission to the card 40 (step 68).

The smart card 40 has an input/output (I/O) port 42 which can include a set of contacts through which programs, data and other communications are provided. The card 40 also includes an installation tool 46 for receiving the contents of the CAP file 16 and preparing the applet for execution on the card 40 (step 70). The installation tool 46 can be implemented, for example, as a Java program and can be executed on the card 40. The card 40 also has memory, including volatile memory such as RAM 50. The card 40 also has ROM 52 and non-volatile memory, such as EEPROM 54. The applet prepared by the controller 44 can be stored in the EEPROM 54.

In one particular implementation, the applet is executed by a virtual machine 49 running on a microprocessor 48 (step 72). The virtual machine 49, which can be referred

to as the Java Card™ Virtual Machine, need not load or manipulate the CAP file 16. Rather, the Java Card Virtual Machine 49 executes the applet code previously stored as part of the CAP file 16. The division of functionality between the Java Card Virtual Machine 49 and the installation tool 46 allows both the virtual machine and the installation tool to be kept relatively small.

In general, implementations and applets written for a resource-constrained platform such as the smart card 40 follow the standard rules for Java platform packages. The Java Virtual Machine and the Java programming language are described in T. Lindholm et al., The Java Virtual Machine Specification (1997), and K. Arnold et al., The Java Programming Language Second Edition, (1998), which are incorporated herein by reference in their entirety. Application programming interface (API) classes for the smart card platform can be written as Java source files which include package designations, where a package includes a number of compilation units and has a unique name. Package mechanisms are used to identify and control access to classes, fields and methods. The Java Card API allows applications written for one Java Card-enabled platform to run on any other Java Card-enabled platform. Additionally, the Java Card API is compatible with formal international standards such as ISO 7816, and industry-specific standards such as Europay/MasterCard/Visa (EMV).

The smart card platform of the present invention supports dynamically created objects including both class instances and arrays. A class is implemented as an extension or subclass of a single existing class and its members are methods as well as variables referred to as fields. A method declares executable code that can be invoked and that receives a fixed number of values as

arguments. Classes also can define or implement Java interfaces. An interface is a reference type whose members are constants and abstract methods.

Individual instructions stored in the CAP file 16 and subsequently downloaded to the smart card 40 include an 8-bit operation code (opcode) followed by either zero, one or multiple 8-bit operands (FIG. 3A). Some instructions have no operands and consist only of an opcode. The general form of the inner loop of execution of the Java Card Virtual Machine 49 is illustrated in FIG. 3B. When a method is invoked, the Java Card Virtual Machine 49 allocates a frame which has a set of local variables and contains an operand stack. Many of the operation codes discussed below take one or more values from the operand stack of the current frame, operate on them, and return results to the same stack. The operand stack also is used to pass arguments to methods and receive method results.

Values from the operand stack must be operated upon in ways that are appropriate to their types. The Java Card Virtual Machine 49 supports two kinds of data types: primitive types and reference types. The numeric primitive types supported by the Java Card Virtual Machine 49 are: (1) "byte", whose values are 8-bit signed two's complement integers; (2) "short", whose values are 16-bit signed two's complement integers; and, optionally, (3) "int", whose values are 32-bit signed two's complement integers. The Java Card Virtual Machine 49 also supports a "returnAddress" type, whose values are pointers to the operation codes in the instructions for the virtual machine. The reference types supported by the Java Card Virtual Machine 49 are (1) "class" types; (2) "interface" types; and (3) "array" types. Those reference types are the same as the reference types used in the Java Virtual Machine. The Java

Card Virtual Machine 49 is defined in terms of an abstract storage unit, which can be referred to as a word, which is sufficiently large to hold a value of the type "byte," "short," "reference," or "returnAddress." Two words are sufficiently large to hold a value of the type "int." Multiple-byte operand data is encoded in big-endian order, in other words, with the high-order byte first.

Various keywords, which cannot be used as identifiers or names of declared entities, are supported by the Java Card Virtual Machine 49. A list of the supported keywords is provided in the attached Appendix at page 11. The function and use of those keywords is the same as the corresponding keywords in the Java programming language.

The operation codes which form the executable program stored in the method component 20 of the CAP file 16 are designed to use the same semantics as that used in the class files 10 written in the Java language. Thus, for example, mathematical results and class hierarchies are preserved when the converter 14 transforms the Java class files 10 into the CAP file 16. Nevertheless, as will be evident from the following description, a sequence of instructions that can be executed by the Java Card Virtual Machine 49 differs from programs intended solely to be run by a system incorporating the Java Virtual Machine. Some of the differences are due to the more limited support of data types present in the instruction set discussed below. Other differences result from the fact that the instruction set discussed below is designed to be executable by a virtual machine residing on a resource-constrained device. Some details of the instruction set are intended to optimize the size or performance of either the Java Card Virtual Machine 49 or the programs running on it. Such details include inlining constant pool data directly into the operation

codes or operands, adding multiple versions of a particular instruction to handle different data types, creating composite instructions for operations on the current object, and explicitly handling 16-bit arithmetic.

Referring to FIGS. 4A and 4B, an exemplary instruction set is provided for programs to be executed by the Java Card Virtual Machine 49. Each instruction is identified by a corresponding operation code (opcode) mnemonic and numerical representation. With the exception of two reserved opcodes, impdep1 and impdep2, all of the opcodes typically can be used in a CAP file such as the CAP file 16. The instructions corresponding to the two reserved opcodes provide backdoors or traps to implementation-specific functionality implemented in software and hardware, respectively. Accordingly, the two reserved opcodes typically do not properly appear in the CAP file 16. They are typically used only in representations of programs that were placed on the smart card 40 by means other than receipt of a CAP file.

As previously mentioned, each instruction includes an operation code followed by zero, one, or more operands. In other words, the instructions have the following general format:

operation code
operand1
operand2
. . .

Each word in the instruction format represents a single 8-bit byte or "bytecode." The instruction's opcode is its numeric representation. Each instruction also has a corresponding mnemonic which is its name. However, only the numeric representation is present in the virtual machine code in a CAP file such as the CAP file 36. Detailed

explanations of each instruction including its function and effect on the operand stack appear in the attached Appendix at pages 97 through 215.

Each data manipulation instruction is specific to a particular data type. The instruction set corresponding to the operation codes listed in FIG. 4A supports a subset of the features supported by the Java programming language. By supporting many, although not all, of the features of the Java language and by using the same semantics as the Java class files 10, platform-independent virtual machine code can be written to be executed by the smart card 40 or other resource-constrained device.

As mentioned above, the instruction set for the Java Card Virtual Machine inlines certain data, which would otherwise appear as part of the constant pool 18, directly into the operation codes or operands. Thus, the instruction set itself incorporates certain information that would otherwise be stored in and obtained from a constant pool if one were using the Java class file format. Thus, when the one or more Java class files 10 are converted to the CAP file 16, at least some references to a constant pool are transformed to inline data in the bytecodes associated with the CAP file.

For example, if the virtual machine 49 supports the data type "int," then the "iipush" operation code can be used to push an integer value onto the operand stack. The general format for the "iipush" instruction is illustrated in FIG. 6A, and the format of a corresponding "ldc" instruction from the Java class file format is shown in FIG 6B. The "ldc" instruction includes the operand "index" which is an unsigned byte that is an index into a constant pool. In contrast, the "iipush" instruction, which is executable by the Java Card Virtual Machine 49, eliminates

the need to refer to the constant pool when executing that instruction. Although the "iipush" instruction includes four operands, thereby increasing the length of the instruction, the slightly longer program can be offset by the savings in memory space which is achieved by eliminating the need to store additional information in the constant pool 18.

Similarly, the "checkcast" operation code can be used to check whether an object is of a particular type. The general format for the "checkcast" instruction for the Java Card Virtual Machine 49 is illustrated in FIG. 7A, and the format of a corresponding "checkcast" instruction from the Java class file format is shown in FIG 7B. The data type for the Java Card Virtual Machine 49 has been inlined directly into the instruction, in contrast to the corresponding Java instruction in which the data type is obtained from a constant pool. By inlining some of the information directly into the instruction set, the size of the constant pool 18 that is stored in the CAP file 16 can be reduced.

The foregoing examples illustrate how the instruction set for the Java Card Virtual Machine 49 inlines some information directly into an operand. In some cases, an additional form of inlining is provided by inlining information that would otherwise be stored in the constant pool 18 directly into an operation code. Thus, for example, the instruction set for the Java Card Virtual Machine adds multiple versions of several instruction to handle different data types so that those instructions appear as members of a family of related instructions which share a single description, format and operand stack diagram. Each instruction in such a family of instructions implicitly specifies the data type in the operation code itself. The

table in FIG. 5 provides a list of the data types which are supported by instructions that exist for multiple data types. Wide and composite forms of instructions are not listed. Referring to FIG. 5, a specific instruction, with the data type incorporated into the operation code, is obtained by replacing the "T" in the instruction template in the opcode column by the letter representing the type in the type column. Where the column for a particular instruction is left blank, then no instruction exists supporting the particular operation on that data type. For example, there is a "load" instruction for the data type "short," but there is no "load" instruction for the data type "byte."

With instructions that implicitly incorporate the data type into the operation code, the program can operate more quickly and with less data on the smart card 40 than would otherwise be required. Those advantages arise because the data type is directly encoded in the instructions rather than being obtained from an entry in the constant pool. For example, consider the family of "getfield_T" instructions, which includes the instructions "getfield_a," "getfield_b," "getfield_s" and "getfield_i." The general format of the "getfield_T" instructions for use with the Java Card Virtual Machine 49 is illustrated in FIG. 8A, which contrasts with the format of the corresponding "getfield" instruction in the Java class file format as shown in FIG. 8B. In the instructions for the Java Card Virtual Machine 49 (FIG. 8A), the data type has been inlined not only into the instruction, but it has been inlined directly into the operation code. On the one hand, such features can reduce the amount of information stored in the CAP file 16 and also can reduce the number of operands required for the particular instruction. On the other hand, those features expand the number of distinct operation codes.

Whereas the type of inlining discussed with respect to the "iipush" and "checkcast" opcodes can be advantageous for instructions that tend to be less frequently used, the type of inlining discussed with respect to the "getfield_t" family of instructions can be advantageous particularly for instructions that tend to be used more frequently.

The foregoing examples illustrate how the instruction set for the Java Card Virtual Machine 49 inherently inlines certain information. Another form of inlining information can occur when the CAP file 16 is downloaded to the smart card 40, as explained below.

The installation tool 46 on the smart card 40 can be platform-specific and allows the actual storage of the contents of the CAP file 16 to be determined based on the particular platform receiving and preparing the virtual machine code for execution. Thus, in some implementations, the CAP file 16 may be stored on the smart card 40, or other resource-constrained device, in a manner that differs from the manner in which it was received by the smart card. For example, in some cases, when the CAP file 16 is installed on the card 40, the installation tool 46 can link the contents of the CAP file so that the size of the constant pool 18 can be reduced, and in some cases, so that the constant pool need not be retained or stored on the card. That can be accomplished by converting the constant pool indices that appear as part of the code in the CAP file 18 to the corresponding data at the time of installation, as illustrated in FIGS. 9A and 9B. For example, an index to the constant pool 16 can be replaced by an index to the appropriate field in the object. Thus, the virtual machine code stored on the card 40 will already have the data incorporated within it prior to the time of execution. The virtual machine code, with the constant pool 18 removed,

reduces some of the indirection inherent in a program which uses a constant pool. The amount of memory required to store the bytecodes on the smart card 40 can, therefore, be reduced, and the execution time for the program also can be reduced. Of course, in other implementations, the installation tool 46 may retain the constant pool 18 when the CAP file 16 is downloaded to the smart card 40.

As previously mentioned, the instruction set for the Java Card Virtual Machine also includes composite instructions for performing operations on the current object. In other words, some of the instructions that are executable by the Java Card Virtual Machine 49 allow multiple instructions to be collapsed into a single instruction. In particular, instructions that include a "this" operation, such as the family of "getfield_T_this" instructions and the family of "putfield_T_this" instructions, effectively concatenate multiple instructions. In general, the "this" operation operates on the current object. For example, to fetch a field from the current object, one could use a combination of the "aload_0" instruction and a "getfield_a" instruction as shown in FIG. 10A. Alternatively, one can use the single instruction "getfield_T_this" as illustrated in FIG. 10B. Use of the latter instruction can result in a smaller and faster program code. As previously noted, such features are particularly advantageous in resource-constrained devices such as the smart card 40.

The instruction set for the Java Card Virtual Machine also handles 16-bit arithmetic explicitly. To illustrate how 16-bit arithmetic is handled, consider a situation in which "a," "b" and "c" have been declared as "short" type variables, and the expression "c = (short) a + b;" is to be compiled. The bytecodes written in the Java

class file format are shown in FIG. 11A. As can be seen from FIG. 11A, five opcodes are used to load the values "a" and "b," to add the values "a" and "b," to convert the resulting integer type into a short type, and to store the result. In contrast, only four opcodes are needed to obtain and store the result using the instruction set for the Java Card Virtual Machine 49 which obviates the need to convert the integer type result into a short type. Furthermore, in addition to using fewer bytecodes, the size of the stack can be reduced by as much as fifty percent because the Java Card Virtual Machine operates on 16-bit quantities rather than 32-bit quantities.

An object-oriented, verifiable instruction set is, therefore, provided and allows a file with virtual machine bytecode to be stored on a computer-readable medium. Such a file can be downloaded to the resource-constrained device so that the bytecode can be executed by the resource-constrained device.

Although a virtual machine 49 running on a microprocessor 48 has been described as one implementation for executing the bytecodes on the smart card 40, in alternative implementations, an application-specific integrated circuit (ASIC), or a combination of hardware and firmware can be used as a controller for executing downloaded code instead.

Furthermore, although the invention can be implemented using the operation codes listed in FIGS. 4A and 4B, other operation codes and corresponding instruction sets having certain characteristics are suited for implementing the invention as well. Such characteristics include verifiability, type safety, pointer safety, object-oriented, dynamically linked, virtual machine-based, platform-independence, and use of the same semantics as the Java

language, although not all of those characteristics need to be present in a particular implementation.

As previously discussed, the Java Card instruction set can be used with a variety of different resource-constrained devices, some of which are listed in FIG. 12.

Other implementations are within the scope of the following claims.

What is claimed is: